# FINANCIAL CRIMES AND MONEY LAUNDERING

#### K. MUJAKAR LECTURER IN COMMERCE P.V.K.N GOVT. COLLEGE,, CHITTOOR.

## ABSTRACT

Money laundering and financial crimes are an activity which is common in all areas. This has been done by cyber crime fraudersters and exploiting the general public, as well as banks, and others. Due to this it damages to many, and getting loss to entire global. Now-a-days, its crime has been increasing very enormous. So, govt. of India has been taken the following measures to controlling and monitoring it. In order to prevent it by passing the bill in parliament, this paper deals with introduction to AML, its features of financial crimes and Anti-money laundering and methods of laundering, and process of money laundering, the trends of money laundering in local, regional and at global level also, and its recommendations and its conclusions. Money laundering is the illegal process of concealing the origins of money obtained illegally by passing it through a complex sequence of bank transfers or commercial transactions. One of the problems of criminal activities is accounting for the proceeds without raising the suspension of law enforcement agencies. India's promising position as a financial centre and its system of informal cross border money flows makes the country's susceptibility to money laundering. Some frequent sources of illegitimate earnings in India are narcotics trafficking, corruption, income tax evasion etc. Combating money laundering is the most important task for the financial sector. For India, to diminish informal money transfer channels, it needs to fortify enforcement around the important areas - responsibility of management in Anti Money Laundering (AML) policies, scrutinizing of AML systems, adoption of appropriate 'Know Your Customer' norms, transaction monitoring, staff training towards regulation compliance

# **KEYWORDS:** FINANCIAL CRIMES, AML, **TRAFFICKING, CORRUPTION, TAX EVASION,** NARCOTICS, REGULATION COMPLIANCE.

**INTRODUCTION**: - The prevention of money laundering Act, 2002 came into force with effect from 01.07.2005. it extends to whole of India.

The PMLA and rules notified there under impose obligation on banking companies, financial institutions and intermediaries and persons carrying on designated business (or) profession to verify identify of clients, maintain records and furnish information to FIU-IND.

PMLA is an act to prevent money laundering and to provide for confiscation of property derived from or involved in money-laundering and for matters connected therewith or incidental thereto.

Money Laundering is the illegal process of concealing the origin of money obtained illegally by passing it through a complete complex sequence of banking transfers or commercial transactions.

One of the Problem of criminal activities is accounting for the proceeds without raising the suspicion of law enforcement agencies.

Considerable time and effort may be put into strategies which enable the safe use of those proceeds without raising unwanted suspicion.

Implementing such strategies is generally called money laundering. After money has been laundered it can be used for legitimate purpose.

Many jurisdictions have setup sophisticated financial and other monitoring systems to enable law enforcement agencies detect suspicious transactions or activities, and many have set-up international co-operative arrangement to assist each other in these endeavors.

In a no. of legal and regulations systems, the term money laundering has become conflated with other forms of financial and business crime, and is sometimes used more generally to include misuse of the financial system (involving things such as securities, digital currencies, credit cards and traditional currencies) including terrorism financing and evasion of international sanctions.

Most anti-money laundering laws openly conflate money laundering (which is concerned with source of funds) with terrorism financing (which is concerned with destination of funds) when regulating financial system.

Some countries treat obfuscation of sources of money as also constituting money laundering, whether it is intentional or by merely using financial systems or services that do not identify or track sources or destinations. Other countries define money laundering such a way to include money from activity that would have been a crime in that country, even if the activity was legal where the actual conduct occurred.

**.** 

#### According to the United States Treasury Department:

Money laundering is the process of making illegally-gained proceeds (i.e., "dirty money") appear legal (i.e., "clean"). Typically, it involves three steps: placement, layering, and integration. First, the illegitimate funds are furtively introduced into the legitimate financial system. Then, the money is moved around to create confusion, sometimes by wiring or transferring through numerous accounts. Finally, it is integrated into the financial system through additional transactions until the "dirty money" appears "clean".

**Offence of money laundering**: - According to **section 3** whosoever directly or indirectly attempts to indulge or knowingly asset or unknowingly is party or is actually involved in any process or activity connected with proceeds with crime namely

- a) Concealment or
- b) Possession or
- c) Acquisition
- d) Projecting as Untained property or
- e) Claiming as Untained property

**Section 4-punishment for money laundering** whoever commits the offence of money laundering shall be punishable with rigorous imprisonment for a team which shall not be less than three years but which may extend to 7 years and shall also liable to fine

Provided that where the proceeds of crime involved in money laundering relates to any offence specified under paragraph 2 of part A of the schedule, the provisions of their section shall effect as if for the words "which may extend to 7 years", the words "which extended to 10 years" had been substituted.

### Section 26 Appeals to Appellate Tribunal: -

(1) Save as otherwise provided in sub-section (3), the Director or any person aggrieved by an order made by the Adjudicating Authority under this Act, may prefer an appeal to the Appellate Tribunal.

(2) Any reporting entity aggrieved by any order of the Director made under sub-section (2) of section 13, may prefer an appeal to the Appellate Tribunal.

(3) Every appeal preferred under sub-section (1) or sub-section (2) shall be filed within a period of forty-five days from the date on which a copy of the order made by the Adjudicating Authority or Director is received and it shall be in such form and be accompanied by such fee as may be prescribed:

Provided that the Appellate Tribunal after giving an opportunity of being heard entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

(4) On receipt of an appeal under sub-section (1) or sub-section (2), the Appellate Tribunal may, after giving the parties to the appeal an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

(5) The Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned Adjudicating Authority or the Director, as the case may be.

(6) The appeal filed before the Appellate Tribunal under sub-section (1) or sub-section (2) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of filing of the appeal.

<u>Section 41 Civil Court not to have jurisdiction</u>-No civil court shall jurisdiction to entertain any suit or proceeding in respect of any matter which the director, an Adjudicating Authority or the Appellate Tribunal is empowered by or under this act to determine and no Injuction shall be granted by any court or other authority in respect of any action taken in pursuance of any power conferred by or under this act.

<u>Section-42 Appeal to High court</u>: Any person Aggrieved by any decision or order of the appellate tribunal may file an appeal to the high court within 60 days from the date of communication of the decision of the decision or order of the appellate tribunal to him or any question of law or fact arising out such order.

Provided that the high court may, if it is satisfied that the appellate was prevented by sufficient cause from filing the appeal within a said a period, allow it to be filed within a further period not exceeding 60 days.

- 1. The high court within the jurisdiction of which the aggrieved party ordinarily resides or carries on business or personally works for gain:
- 2. Where the CG is the aggrieved party, the high court within the jurisdiction of which the respondent or in a case where there are more than one respondent, any one of respondent ordinarily resides or carry on business or personally works for gain.

<u>Section-69 Recovery of fine or penalty</u>: - where any fine or penalty imposed on any person under section 13 or under section 63 is not paid within 6 months from the date of imposition of fine or penalty, the director or any other officer-authorized by him. On this behalf may proceed to recover the amount from the said person in the same manner as prescribed in schedule II of I.T Act, 1961 for the recovery of arrears and he or any officer authorized by him in this behalf shall have all the powers of the tax recovery officer mentioned in the said schedule for the purpose.

#### Methods of money laundering

Money laundering can take several forms, although most methodology can be categorized into one of a few types. These include "bank methods, smurfing [also known as structuring], currency exchanges, and double-invoicing"

**<u>Structuring</u>**: Often known as <u>*smurfing*</u>, is a method of placement whereby cash is broken into smaller deposits of money, used to defeat suspicion of money laundering and to avoid anti-money laundering reporting requirements.

A sub-component of this is to use smaller amounts of cash to purchase bearer instruments, such as money orders, and then ultimately deposit those, again in small amounts.

- **Bulk cash smuggling:** This involves physically smuggling cash to another jurisdiction and depositing it in a financial institution, such as an <u>offshore bank</u>, with greater <u>bank secrecy</u> or less rigorous money laundering enforcement.
- <u>Cash-intensive businesses</u>: In this method, a business typically expected to receive a large proportion of its revenue as cash uses its accounts to deposit criminally derived cash. Such enterprises often operate openly and in doing so generate cash revenue from incidental legitimate business in addition to the illicit cash. In such cases the business will usually claim all cash received as legitimate earnings. Service businesses are best suited to this method, as such enterprises have little or no variable costs and/or a large ratio between revenue and variable costs, which makes it difficult to detect discrepancies between revenues and costs. Examples are parking structures, strip clubs, tanning salons, car washes, arcades, bars, restaurants, and casinos.
- <u>**Trade-based laundering**</u>: This method is one of the newest and most complex forms of money laundering. This involves under- or over-valuing <u>invoices</u> to disguise the movement of money. For example, the art market has been accused of being an ideal vehicle for money laundering due to several unique aspects of art such as the subjective value of art works as well as the secrecy of auction houses about the identity of the buyer and seller.
- <u>Shell companies and trusts</u>: Trusts and shell companies disguise the true owners of money. Trusts and corporate vehicles, depending on the jurisdiction, need not disclose their true owner. Sometimes referred to by the slang term *rathole*, though that term usually refers to a person acting as the fictitious owner rather than the business entity.
- <u>**Round-tripping**</u>: Here, money is deposited in a <u>controlled foreign corporation</u> offshore, preferably in a <u>tax</u> <u>haven</u> where minimal records are kept, and then shipped back as a <u>foreign direct investment</u>, exempt from taxation. A variant on this is to transfer money to a law firm or similar organization as funds on account of fees, then to cancel the retainer and, when the money is remitted, represent the sums received from the lawyers as a legacy under a will or proceeds of litigation.
- <u>Bank capture</u>: In this case, money launderers or criminals buy a controlling interest in a bank, preferably in a jurisdiction with weak money laundering controls, and then move money through the bank without scrutiny.
- <u>Casinos</u>: In this method, an individual walks into a casino and buys chips with illicit cash. The individual will then play for a relatively short time. When the person cashes in the chips, they will expect to take payment in a check, or at least get a receipt so they can claim the proceeds as gambling winnings.
- Other gambling: Money is spent on gambling, preferably on high odds games. One way to minimize risk with this method is to bet on every possible outcome of some event that has many possible outcomes, so no outcome(s) have short odds, and the bettor will lose only the vigorish and will have one or more winning bets that can be shown as the source of money. The losing bets will remain hidden.
- <u>Black salaries</u>: A company may have unregistered employees without written contracts and pay them cash salaries. Dirty money might be used to pay them.
- <u>Tax amnesties</u>: For example, those that legalizes unreported assets and cash in tax havens.
- <u>**Transaction Laundering**</u>: When a merchant unknowingly processes illicit credit card transactions for another business. It is a growing problem and recognized as distinct from traditional money laundering in using the payments ecosystem to hide that the transaction even occurred (e.g. the use of fake front websites). Also known as "undisclosed aggregation" or "factoring".

#### **Digital electronic money**

In theory, <u>electronic money</u> should provide as easy a method of transferring value without revealing identity as untracked banknotes, especially wire transfers involving anonymity-protecting numbered bank accounts. In practice, however, the record-keeping capabilities of Internet service providers and other network resource maintainers tend to frustrate that intention. While some <u>crypto currencies</u> under recent development have aimed to provide for more possibilities of transaction anonymity for various reasons, the degree to which they succeed— and, in consequence, the degree to which they offer benefits for money laundering efforts—is controversial. Solutions such as <u>ZCash</u> and Monero are examples of crypto currencies that provide unlinkable anonymity via proofs and/or obfuscation of information (<u>ring signatures</u>). Such currencies could find use in online illicit services.

In 2013, Jean-Loup Richet, a research fellow at <u>ESSEC</u> ISIS, surveyed new techniques that cybercriminals were using in a report written for the <u>United Nations Office on Drugs and Crime</u>. A common approach was to use a <u>digital currency exchanger</u> service which converted dollars into a digital currency called <u>Liberty Reserve</u>, and could be sent and received anonymously. The receiver could convert the Liberty Reserve currency back into cash for a small fee. In May 2013, the US authorities shut down Liberty Reserve charging its founder and various others with money laundering.

Another increasingly common way of laundering money is to use online gaming. In a growing number of online games, such as <u>Second Life</u> and <u>World of Warcraft</u>, it is possible to <u>convert money into virtual goods</u>, <u>services</u>, or <u>virtual cash</u> that can later be converted back into money.

To avoid the usage of decentralized digital money such as <u>Bitcoin</u> for the profit of crime and corruption, Australia is planning to strengthen the nation's anti-money laundering laws. The characteristics of Bitcoin—it is completely deterministic, protocol based and cannot be censored—make it possible to circumvent national laws using services like <u>Tor</u> to obfuscate transaction origins. Bitcoin relies completely on cryptography, not on a central entity running under a <u>KYC</u> framework. There are several cases in which criminals have cashed out a significant amount of Bitcoin after ransom ware attacks, drug dealings, cyber fraud and gunrunning.

#### **Reverse money laundering**

Reverse money laundering is a process that disguises a legitimate source of funds that are to be used for illegal purposes. It is usually perpetrated for the purpose of financing terrorism but can be also used by criminal organizations that have invested in legal businesses and would like to withdraw legitimate funds from official circulation. Unaccounted cash received via disguising financial transactions is not included in official financial reporting and could be used to evade taxes, hand in bribes and pay "under-the-table" salaries. For example, in an affidavit filed on 24 March 2014 in United States District Court, Northern California, San Francisco Division, FBI special agent Emmanuel V. Pascau alleged that several people associated with the Chee Kung Tong organization, and California State Senator Leland Yee, engaged in reverse money laundering activities.

The problem of such fraudulent encashment practices (*obnalichka* in Russian) has become acute in Russia and other countries of the former Soviet Union. The Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) reported that the Russian Federation, Ukraine, Turkey, Serbia, Kyrgyzstan, Uzbekistan, Armenia and Kazakhstan have encountered a substantial shrinkage of tax base and shifting money supply balance in favor of cash.

These processes have complicated planning and management of the economy and contributed to the growth of the <u>shadow economy</u>.

#### Magnitude

Many regulatory and governmental authorities issue estimates each year for the amount of money laundered, either worldwide or within their national economy. In 1996, a spokesperson for the IMF estimated that 2–5% of the worldwide global economy involved laundered money. The <u>Financial Action Task Force on Money</u> <u>Laundering</u> (FATF), an intergovernmental body set up to combat money laundering, stated, "Due to the illegal nature of the transactions, precise statistics are not available and it is therefore impossible to produce a definitive estimate of the amount of money that is globally laundered every year. The FATF therefore does not publish any figures in this regard." Academic commentators have likewise been unable to estimate the volume of money with any degree of assurance.[9] Various estimates of the scale of global money laundering are sometimes repeated often enough to make some people regard them as factual—but no researcher has overcome the inherent difficulty of measuring an actively concealed practice.

Regardless of the difficulty in measurement, the amount of money laundered each year is in the <u>billions</u> of US dollars and poses a significant policy concern for governments.[9] As a result, governments and international bodies have undertaken efforts to deter, prevent, and apprehend money launderers. Financial institutions have likewise undertaken efforts to prevent and detect transactions involving dirty money, both as a result of government requirements and to avoid the reputational risk involved. Issues relating to money laundering have existed as long as there have been <u>large scale criminal enterprises</u>. Modern anti-money laundering laws have developed along with the modern <u>War on Drugs</u>. In more recent times anti-money laundering legislation is seen as adjunct to the financial crime of <u>terrorist financing</u> in that both crimes usually involve the transmission of funds through the financial system (although money laundering relates to where the money has come *from*, and terrorist financing relating to where the money is going *to*).

Transaction laundering is a massive and growing problem. Finextra estimated that transaction laundering accounted for over \$200 billion in the US in 2017 alone, with over \$6 billion of these sales involving illicit goods or services, sold by nearly 335,000 unregistered merchants.

Stages of money laundering: - There are three stages of money laundering are:

- 1. <u>Placement stage</u>: The placement stage represents the initial entity of the "dirty" cash or proceeds of crime into the financial system. Generally serves two purposes
- a) It relieves the criminal of holding and guarding large amounts of bulky of cash; and
- b) It places the money into the legitimate financial system. It is during the placement stage that money laundering are the most vulnerable to being caught. This is due to fact placing large amounts of money (cash) into the legitimate financial system may raise suspicions of officials.

This placement of the proceeds of crime can be done in a no. of ways.

# For example: cash could be packed into a suitcase and smuggled to a country, or the launderer could use Smurfs to defeat reporting threshold laws and avoid suspicion. Some other common methods include:

- Loan repayment; Repayment of loans or credit cards with illegal proceeds
- Seambling: Purchase of gambling chips or placing bets on sporting events
- Currency smuggling: The physical movement of illegal currency or monetary instruments over the border.
- **<u>Currency exchange</u>**: Purchasing of foreign money with illegal funds through foreign exchanges
- Blending funds: using legitimate cash focused business to co-mingle dirty funds with day's legitimate sales receipts.

This environment has resulted in a situation where officials in these jurisdictions are either unwilling due to regulations or refuse to cooperate in requests for assistance during international money laundering investigations.

To combat this and other international impediments to effective money laundering investigations, many like-minded countries have met to develop, coordinate, and share model legislation, multi-lateral agreements trends, and intelligence and other information

<u>**The layering Stage</u>**: - Sometimes called as (structuring). The layering stage is most complex and often entails the international movement of funds. The primary purpose of the stage is to separate the illicit money from its source. This is done by sophisticated layering of financial transactions that obscure that audit trail and server the link with original crime.</u>

During this stage, for example the money laundering may begin by moving funds electronically from one country to another, then divide them into investments placed in advanced financial options or overseas markets, constantly moving them to elude detection each time, exploiting loopholes or discrepancies in legislation and taking advantage of delays in judicial or police cooperation.

Integration stage: - This is final stage of money laundering:

Where the money is returned to the criminal from what seem to be legitimate sources having been placed initially as cash and layered through a no. of financial transactions, the criminal proceeds are new fully integrated into the financial system and can be used for any purpose.

There are many different ways in which the laundered money can be integrated back with the criminal, however, the major objective at this stage is to reunite the money with the criminal in a manner that does not draw attention and appears to result from a legitimate source for example, the purchase of property, art work, jewelers or high-end automobiles are common ways for the launder to enjoy their illegal profits without necessary drawing attention to themselves.

#### Anti-Money laundering measures by region: -

Section-12(1), describes the obligations that banks other financial institutions and intermediaries have to

- a) Maintain records that detail the nature and value of transactions, whether such transactions comprise a single transaction or a series of connected transactions, and where these transactions take place within a month
- b) Furnish information on transactions referred to in Clause (a) to the director within the time prescribed, including records of the identity of all its clients.

Section 12(2) prescribes that the records referred to in Sub-Section (1) as mentioned above, must be maintained for 10 years after the transactions finished. It is handled by the I.T Department. The provisions of the act are frequently reviewed and various amendments have been

Passed from time to time, "Most Money Laundering Activities in India are through political parties, corporate companies the shares market. These are investigated by the enforcement Directorate and the Income Tax Department"

Bank Accountants must record all transactions over Rs. 1 million and maintain such records for 10 years.

**Banks must also Cash Transactions Reports (CTRs)** and suspicious transactions reports over RS. 1 million within 7 days of initial suspicion, they must submit report to Enforcement Directorate and Income Tax Department.

#### 12A. Access to information.—

(1) The Director may call for from any reporting entity any of the records referred to in section 11A, sub-section (1) of section 12, sub-section (1) of section 12AA and any additional information as he considers necessary for the purposes of this Act.

(2) Every reporting entity shall furnish to the Director such information as may be required by him under subsection (1) within such time and in such manner as he may specify.

(3) Save as otherwise provided under any law for the time being in force, every information; sought by the Director under sub-section (1), shall be kept confidential.

#### 12AA.(1) Every reporting entity shall, prior to the commencement of each specified transaction,—

(a) verify the identity of the clients undertaking such specified transaction by authentication under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 in such manner and subject to such conditions, as may be prescribed: Provided that where verification requires authentication of a person who is not entitled to obtain an Aadhaar number under the provisions of the said Act, verification to authenticate the identity of the client undertaking such specified transaction shall be carried out by such other process or mode, as may be prescribed; (b) take additional steps to examine the ownership and financial position, including sources of funds of the client, in such manner as may be prescribed;

(c) take additional steps as may be prescribed to record the purpose behind conducting the specified transaction and the intended nature of the relationship between the transaction parties.

(2) Where the client fails to fulfil the conditions laid down under sub-section (1), the reporting entity shall not allow the specified transaction to be carried out.

(3) Where any specified transaction or series of specified transactions undertaken by a client is considered suspicious or likely to involve proceeds of crime, the reporting entity shall increase the future monitoring of the business relationship with the client, including greater scrutiny or transactions in such manner as may be prescribed.

(4) The information obtained while applying the enhanced due diligence measures under sub-section (1) shall be maintained for a period of five years from the date of transaction between a client and the reporting entity.

Explanation: - For the purposes of this section, "specified transaction" means—.

(a) any withdrawal or deposit in cash, exceeding such amount;

(b) any transaction in foreign exchange, exceeding such amount;

(c) any transaction in any high value imports or remittances;

(d) such other transaction or class of transactions, in the interest of revenue or where there is a high risk or money-laundering or terrorist financing, as may be prescribed.

Section 56: Agreement with foreign countries

Section 73 & 75: it has power to make rules and power to make difficulties

<u>Recommendations and conclusions</u>: here, at present lot of cyber crimes and financial crimes are happening, even though there is a lot of amendments and rules and regulations. Here I want to tell that

- due to lot of rules and sections in our constitution and the loop holes has been increased and the fruadesters are escaping
- to the cyber fraudesters bailment should not be given; if any accused appointed unwontedly by the involvement of other persons without any mistake, then to be put enquiry and take the decisions according to the law
- The apps one of the major problem to create an disturbances in our economic system, so the new apps must not be recommended, even if it is permissible than it should be checked and verified to the public than it should be released, and
- Even in digital economy we are in good position, the hackers are hacking the currency through online mode.
- There should be good awareness programmes about this sections and fines and penalties and imprisonment to the students, general public; so, some what it can be avoided the programmes like a subject about crimes should be in all universities, through conducting of national seminars, national workshops and some of the international conferences and also through major objective is media which at least can be avoided.
- Even though it should be aware to the illiterate public and train to them.
- Due to implementation and training programmes and courses about this the crime can be easily predicted.
- Even though till now, it is in descriptive mode, it should be implemented practical. There should be full support from president and other officials and encourage them; and full powers to be given then only it can be succeeded
- In developed countries there are going speed generation of networks easily, to identify and to recognize crime, but particularly, in India like there should be good network to hack easily.

- The persons like NRIs or Citizens of India who are establishing a new company like software, or Ebusiness before granting a license should be thoroughly checked and give an license and keep regular check-up on existing companies also.
- Still to say that, after cyber crime has been attacked the case should be taken-up in prescribed manner and case to be filed-up within days after attack
- The RTGs, NEFT, SWIFT, CHIPS, CHAPS and other Electronic Fund Transfers Should be more effective and more protective while transferring online currency from one to another and there should be use only authenticated users and still required to be use of Bio-Metrics of persons to use their data information from their systems.
- Finally I am, concluding that, there should be effective disclosure of information to the general public, according to RTI Act, there should be available of information from any sectors.

#### **References**:

- 1) http://www.fiu.gov.in/files/AML\_Legislation/pmla\_2002.html#collapse21
- 2) <u>http://www.en.m.wikipedia.org/wiki/money\_laundering</u>
- 3) <a href="http://www.moneylaundering.ca/public/law/3\_stages\_ML.php">http://www.moneylaundering.ca/public/law/3\_stages\_ML.php</a>
- 4) <u>http://www.igidr.ac.in>conf>money>mfc-12>gujarathi\_medha</u>

